



日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

2000年 1月 7日

出願番号
Application Number:

特願2000-005910

出願人
Applicant(s):

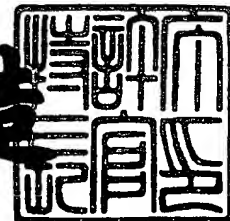
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年11月17日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3095905

【書類名】 特許願

【整理番号】 9900863503

【提出日】 平成12年 1月 7日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 情報携帯処理システム、情報携帯装置のアクセス装置及び情報携帯装置

【請求項の数】 14

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 日下部 進

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 高田 昌幸

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

 【氏名】 佐々木 将央

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100102185

 【弁理士】

 【氏名又は名称】 多田 繁範

 【電話番号】 03-5950-1478

【手数料の表示】

【予納台帳番号】 047267

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9713935

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報携帯処理システム、情報携帯装置のアクセス装置及び情報携帯装置

【特許請求の範囲】

【請求項 1】

ユーザーにより携帯される情報携帯装置を複数の事業者により共用する情報携帯処理システムであって、

前記各事業者固有のファイル鍵情報と所定の管理部門固有の発行者鍵情報とにより前記管理部門で生成されたアクセス鍵情報を用いて、前記各事業者のアクセス装置と前記情報携帯装置とで認証の処理を実行し、

前記情報携帯装置の前記事業者に割り当てられたメモリ空間を前記アクセス装置によりアクセス可能とする

ことを特徴とする情報携帯処理システム。

【請求項 2】

前記事業者のアクセス装置は、

少なくとも前記情報携帯装置に確保するメモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを、前記管理部門固有の第 2 の鍵情報により暗号化して前記管理部門で生成されたファイル登録情報を、前記情報携帯装置に送信し、

前記情報携帯装置は、

前記ファイル登録情報より、前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報と復号し、

該メモリ空間の大きさを特定する情報により前記事業者に割り当てるメモリ空間を設定すると共に、

該メモリ空間と関連付けて前記ファイル鍵情報を記録する

ことを特徴とする請求項 1 に記載の情報携帯処理システム。

【請求項 3】

前記前記管理部門固有の第 2 の鍵情報は、

前記発行者鍵情報であり、

前記ファイル登録情報は、

前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを、前記発行者鍵情報により暗号化した暗号化情報に、前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを付加して生成され、

前記情報携帯装置は、

前記ファイル登録情報の前記メモリ空間の大きさを特定する情報と、前記ファイル登録情報の前記ファイル鍵情報とを前記発行者鍵情報により暗号化して暗号化情報を生成し、該暗号化情報と前記ファイル登録情報の暗号化情報との比較により前記ファイル登録情報の正当性を確認する

ことを特徴とする請求項 2 に記載の情報携帯処理システム。

【請求項 4】

前記事業者のアクセス装置は、

前記情報携帯装置に記録し直す発行者鍵情報を前記情報携帯装置に保持された発行者鍵情報により前記管理部門で暗号化して生成された発行者鍵変更情報を前記情報携帯装置に送信し、

前記情報携帯装置は、

前記発行者鍵変更情報を前記内部に保持した発行者鍵情報により処理して前記記録し直す発行者鍵情報を復号し、

該記録し直す発行者鍵情報により前記内部に保持した発行者鍵情報を更新することを特徴とする請求項 1 に記載の情報携帯処理システム。

【請求項 5】

前記事業者のアクセス装置は、

前記発行者鍵変更情報と共に、対応する前記アクセス鍵情報を前記管理部門より取得する

ことを特徴とする請求項 4 に記載の情報携帯処理システム。

【請求項 6】

ユーザーにより携帯される情報携帯装置を複数の事業者により共用する情報携帯処理システムに適用され、前記情報携帯装置をアクセスする情報携帯装置のアクセス装置であって、

前記情報携帯装置は、

メモリ空間が前記各事業者毎に割り当てられ、

前記情報携帯装置のアクセス装置は、

前記各事業者に固有のファイル鍵情報と所定の管理部門に固有の発行者鍵情報とにより前記管理部門で生成されたアクセス鍵情報により、前記情報携帯装置のアクセスに必要な認証の処理を前記情報携帯装置との間で実行する

ことを特徴とする情報携帯装置のアクセス装置。

【請求項 7】

前記事業者のアクセス装置は、

少なくとも前記情報携帯装置に確保するメモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを前記管理部門に固有の第 2 の鍵情報により前記管理部門で暗号化して生成されたファイル登録情報を前記情報携帯装置に送信して、前記情報携帯装置に対応するメモリ空間を確保する

ことを特徴とする請求項 6 に記載の情報携帯装置のアクセス装置。

【請求項 8】

前記管理部門に固有の第 2 の鍵情報は、

前記発行者鍵情報であり、

前記ファイル登録情報は、

前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを、前記発行者鍵情報により暗号化した暗号化情報に、前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを付加して生成された

ことを特徴とする請求項 7 に記載の情報携帯装置のアクセス装置。

【請求項 9】

前記事業者のアクセス装置は、

前記携帯情報装置に記録し直す発行者鍵情報を前記携帯情報装置に保持された発行者鍵情報により前記管理部門で暗号化して生成された発行者鍵変更情報を前記情報携帯装置に送信して、前記情報携帯装置の内部に保持した発行者鍵情報を更新する

ことを特徴とする請求項 7 に記載の情報携帯装置のアクセス装置。

【請求項 1 0】

前記事業者のアクセス装置は、
前記発行者鍵変更情報と共に、対応する前記アクセス鍵情報を前記管理部門より取得する
ことを特徴とする請求項 9 に記載の情報携帯装置のアクセス装置。

【請求項 1 1】

ユーザーにより携帯され、複数の事業者により共用される情報携帯装置であって、
メモリ空間が前記各事業者毎に割り当てられ、
前記各事業者に固有のファイル鍵情報と、所定の管理部門に固有の発行者鍵情報とを保持し、
所定のアクセス装置より送出された情報を前記ファイル鍵情報、前記発行者鍵情報を用いて処理して処理結果を判定することにより、
該ファイル鍵情報に対応するメモリ空間のアクセスを前記アクセス装置に許可する
ことを特徴とする情報携帯装置。

【請求項 1 2】

少なくとも前記情報携帯装置に確保するメモリ空間の大きさを特定する情報と前記ファイル鍵情報とを前記管理部門に固有の第 2 の鍵情報により暗号化して前記管理部門で生成されたファイル登録情報を、前記事業者のアクセス装置より受信し、
前記ファイル登録情報より、前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報と復号し、
該メモリ空間の大きさを特定する情報により前記事業者にメモリ空間を割り当てると共に、
該メモリ空間と関連付けて前記ファイル鍵情報を記録する
ことを特徴とする請求項 1 1 に記載の情報携帯装置。

【請求項 1 3】

前記管理部門に固有の第 2 の鍵情報は、

前記発行者鍵情報であり、

前記ファイル登録情報は、

前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを、前記発行者鍵情報により暗号化した暗号化情報に、前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを付加して生成され、

前記情報携帯装置は、

前記ファイル登録情報の前記メモリ空間の大きさを特定する情報と、前記ファイル鍵情報とを前記内部に保持した発行者鍵情報により暗号化して暗号化情報を生成し、該暗号化情報と前記ファイル登録情報の暗号化情報との比較により前記事業者のアクセス装置を認証する

ことを特徴とする請求項 1 1 に記載の情報携帯装置。

【請求項 1 4】

前記情報携帯装置に記録し直す発行者鍵情報を前記情報携帯装置に保持された発行者鍵情報により前記管理部門で暗号化して生成された発行者鍵変更情報を前記事業者のアクセス装置より受信し、

前記発行者鍵変更情報を前記内部に保持した発行者鍵情報により処理して前記記録し直す発行者鍵情報を復号し、

該記録し直す発行者鍵情報により前記内部に保持した発行者鍵情報を更新することを特徴とする請求項 1 1 に記載の情報携帯装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、情報携帯処理システム、情報携帯装置のアクセス装置及び情報携帯装置に関し、例えば非接触型の IC カードを用いたシステムに適用することができる。本発明は、管理部門で管理する発行者鍵情報と、事業者に固有のファイル鍵情報によりアクセス鍵を生成して各事業者へ配付し、このアクセス鍵を使用して情報携帯装置をアクセスすることにより、複数の事業者で IC カードを共用することができるようにする。

【 0 0 0 2 】

【従来の技術】

従来、ＩＣカードシステムにおいては、個人が携帯するＩＣカードに各種個人の情報等を記録し、駅の改札、部屋の入退出の管理等に使用するようになされている。

【 0 0 0 3 】

これに対して同種のカード形状の媒体として、例えばプリペイドカード、各店舗が発行するサービス用のカード、各ソフトメーカーが発行するユーザーカード等が利用されるようになされている。

【 0 0 0 4 】

これらのカードにおいては、ＩＣカードを含めて、それぞれ各カードに係るサービスを提供する事業者が個別に発行して利用に供されるようになされている。

【 0 0 0 5 】

【発明が解決しようとする課題】

ところでＩＣカードにおいては、内蔵のメモリに複数のサービスに係る個人情報等を十分に記録可能な容量を確保することができることにより、複数の事業者でＩＣカードを共用することができると考えられる。

【 0 0 0 6 】

このようにすればそれまでカードを発行していた事業者においては、カード発行の負担を軽減することができ、また個々の事業者では獲得困難な多数のユーザーを獲得することもできる。またユーザーにおいては、携帯して管理するカードの枚数を少なくすることができることにより、多数のカードを携帯、管理する煩雑さから開放されることになる。

【 0 0 0 7 】

ところがこのようにＩＣカードを複数の事業者で共用する場合、各事業者毎に、ユーザーの個人情報を秘密化することが必要になる。また各事業者が使用するメモリ空間を時間的にも領域的にも管理する必要がある。

【 0 0 0 8 】

本発明は以上の点を考慮してなされたもので、複数の事業者でＩＣカード等を

共用することができる情報携帯処理システム、情報携帯装置のアクセス装置及び情報携帯装置を提案しようとするものである。

【 0 0 0 9 】

【課題を解決するための手段】

かかる課題を解決するため請求項 1 の発明においては、ユーザーにより携帯される情報携帯装置を複数の事業者により共用する情報携帯処理システムに適用して、各事業者固有のファイル鍵情報と管理部門固有の発行者鍵情報とにより管理部門で生成されたアクセス鍵情報を用いて、各事業者のアクセス装置と情報携帯装置とで認証の処理を実行し、情報携帯装置の事業者に割り当てられたメモリ空間をアクセス装置によりアクセス可能とする。

【 0 0 1 0 】

また請求項 6 の発明においては、情報携帯装置をアクセスする情報携帯装置のアクセス装置に適用して、各事業者固有のファイル鍵情報と管理部門固有の発行者鍵情報とにより所定の管理部門で生成されたアクセス鍵情報により、情報携帯装置のアクセスに必要な認証の処理を情報携帯装置との間で実行する。

【 0 0 1 1 】

また請求項 1 1 の発明においては、情報携帯装置に適用して、各事業者固有のファイル鍵情報と、所定の管理部門固有の発行者鍵情報とを保持し、所定のアクセス装置より送出された情報をファイル鍵情報、発行者鍵情報を用いて処理して処理結果を判定することにより、該ファイル鍵情報に対応するメモリ空間のアクセスをアクセス装置に許可する。

【 0 0 1 2 】

請求項 1 の構成によれば、各事業者固有のファイル鍵情報と管理部門固有の発行者鍵情報とにより所定の管理部門で生成されたアクセス鍵情報を用いて、認証の処理を実行し、情報携帯装置の事業者に割り当てられたメモリ空間をアクセス装置によりアクセス可能とすれば、複数の事業者にメモリ空間を割り振って各事業者が情報携帯装置を共用する場合でも、ファイル鍵情報によりあたかも各事業者固有の情報携帯装置のように、各事業者で情報携帯装置をアクセスすることができる。また所定の事業者に割り当てたメモリ空間に対する他の事業者の

アクセスも防止することができる。さらに発行者鍵情報を管理部門で管理することにより、情報携帯装置の管理については、管理部門で管理することができる。

【 0 0 1 3 】

また請求項 6 の構成によれば、各事業者固有のファイル鍵情報と管理部門固有の発行者鍵情報とにより所定の管理部門で生成されたアクセス鍵情報により、情報携帯装置のアクセスに必要な認証の処理を情報携帯装置との間で実行することにより、発行者鍵により管理部門で許可される者によるアクセスについてだけアクセス可能とすることができ、またファイル鍵により各事業者に対応するメモリ空間を特定することができ、これによりあたかも各事業者固有の情報携帯装置のように、各事業者で情報携帯装置をアクセスすることができる。また所定の事業者割り当てメモリ空間に対する他の事業者のアクセスも防止することができ、さらには発行者鍵情報を管理部門で管理することにより、情報携帯装置の管理については、管理部門で管理することができる。

【 0 0 1 4 】

また請求項 1 1 の構成によれば、各事業者固有のファイル鍵情報と、所定の管理部門固有の発行者鍵情報とを保持し、所定のアクセス装置より送出された情報をファイル鍵情報、発行者鍵情報を用いて処理して処理結果を判定することにより、該ファイル鍵情報に対応するメモリ空間のアクセスを前記アクセス装置に許可することにより、複数の事業者によりメモリ空間をアクセスする場合でも、ファイル鍵情報により各事業者割り当てメモリ空間を特定でき、これによりあたかも各事業者固有の情報携帯装置のように、各事業者で情報携帯装置をアクセスすることができる。また所定の事業者割り当てメモリ空間に対する他の事業者のアクセスも防止することができ、さらには発行者鍵情報を管理部門で管理することにより、情報携帯装置の管理については、管理部門で管理することができる。

【 0 0 1 5 】

【発明の実施の形態】

以下、適宜図面を参照しながら本発明の実施の形態を詳述する。

【 0 0 1 6 】

(1) 第 1 の実施の形態

(1 - 1) 第 1 の実施の形態の構成

図 2 は、本発明の第 1 の実施の形態に係る I C カードシステムを示すブロック図である。この I C カードシステム 1 においては、ユーザー 2 の携帯する I C カード 3 を複数の事業者 4 A、4 B、……の提供するサービスで共用できるように、I C カード 3 の管理部門である発行者 5 で I C カード 3 を発行する。

【 0 0 1 7 】

すなわち発行者 5 は、図 3 に示すように、ユーザーからの直接の代金の支払いにより、又は事業者 4 A、4 B、……を介してのユーザーからの間接的な代金の支払いにより、さらにはユーザーに代えた事業者 4 A、4 B、……による代金の支払いにより、このユーザーに対して I C カード 3 を発行する。なお発行者 5 は、直接に、又は事業者 4 A、4 B、……を介して I C カード 3 をユーザーに発行する。

【 0 0 1 8 】

このとき発行者 5 は、I C カード 3 に発行者鍵を記録して発行する。ここでこの発行者鍵は、発行者 5 に固有の鍵情報であり、発行者 5 が管理する暗号化用及び暗号化解除用の鍵情報である。I C カードシステム 1 では、この発行者鍵と各事業者 4 A、4 B、……に固有の鍵情報であるファイル鍵情報とを使用して I C カード 3 をアクセスすることにより、I C カード 3 を発行者により管理して、かつ各事業者 4 A、4 B、……で I C カード 3 を共用できるようになされている。

【 0 0 1 9 】

発行者 5 は、例えばコンピュータ等の管理用の端末装置 6 によりこの発行者鍵を I C カード 3 に記録する。また発行者 5 は、事業者 4 A、4 B、……との契約等により、各事業者 4 A、4 B、……が提供するサービスでこの I C カード 3 を利用可能とする場合、端末装置 6 により構成されるファイル登録情報作成部 7、アクセス鍵合成部 8 によりファイル登録情報、アクセス鍵を作成し、これらファイル登録情報、アクセス鍵を各事業者 4 A、4 B、……に渡す。

【 0 0 2 0 】

ここでファイル登録情報は、各事業者 4 A、4 B、……が自己のサービスに使用可能に、I C カード 3 にメモリ空間を確保するための情報であり、I C カード 3 では、このファイル登録情報の受信により対応するメモリ空間を確保する。またアクセス鍵は、このようにして確保したメモリ空間のアクセスにおける認証に使用する情報であり、結果的に、各事業者に割り当てられたファイル鍵情報と発行者鍵とにより認証の処理を実行する情報である。

【 0 0 2 1 】

ここで図 5 に示すように、ファイル登録情報作成部 7 は、第 1 の暗号化部 7 A により発行者鍵を用いてファイル名、ファイルサイズ情報を暗号化した後、排他的論理和演算部 7 B によりこの暗号化結果とファイル鍵情報との排他的論理和を演算する。さらに第 2 の暗号化部 7 C により発行者鍵を用いてこの排他的論理和の演算結果を暗号化してチェックコードを生成する。

【 0 0 2 2 】

ここでファイル名は、各事業者 4 A、4 B、……に割り当てられるファイル名であり、各事業者 4 A、4 B、……においては、このファイル名により確保された I C カード 3 のメモリ空間を自己のサービスに利用できるようなされている。かくするにつき各事業者 4 A、4 B、……は、自己のサービスに割り当てられたメモリ空間をアクセスする場合には、このファイル名により I C カード 3 をアクセスすることになる。

【 0 0 2 3 】

ファイルサイズは、このファイル名によるファイルの大きさを示し、各事業者 4 A、4 B、……に確保される I C カード 3 のメモリ空間の大きさを示す。ファイル鍵情報は、各ファイル名の領域をアクセスを求めるのに必要な鍵情報である。チェックコードは、ファイル登録情報の正当性をチェックするために使用されるコードである。

【 0 0 2 4 】

ファイルサイズは、事業者 4 A、4 B、……に使用を許可する I C カード 3 のメモリ領域の大きさにより、発行者により設定される。これに対してファイル名

、ファイル鍵情報は、事業者 4 A、4 B、……からの発行者 5 への通知により、又は事業者 4 A、4 B、……と発行者 5 との話し合い等により、各事業者 4 A、4 B、……にそれぞれ固有に、かつ各事業者 4 A、4 B、……がそれぞれ自己のファイル登録情報に割り当てられたファイル名、ファイル鍵情報のみを知り得るよう設定される。

【 0 0 2 5 】

ファイル登録情報作成部 7 は、これらファイル名の情報、ファイルサイズの情報、ファイル鍵情報、チェックコードを所定順序により配列してファイル登録情報を作成する。

【 0 0 2 6 】

アクセス鍵合成部 8 は、図 6 に示すように、暗号化部 8 A において、ファイル鍵を発行者鍵により暗号化してアクセス鍵を生成する。

【 0 0 2 7 】

発行者 5 は、事業者 4 A、4 B、……との間で契約の継続が更新されると、図 7 に示すように、発行者鍵変更情報作成部 9 により発行者鍵変更情報を作成し、この発行者鍵変更情報に対応する事業者 4 A、4 B、……に渡す。これにより発行者 5 は、契約の更新周期を単位とした一定周期により I C カード 3 に記録された発行者鍵を更新する。またこのようにして新たに I C カード 3 に記録する発行者鍵を用いたアクセス鍵合成部 8 の処理により、新たなアクセス鍵を作成して事業者 4 A、4 B、……に渡す。

【 0 0 2 8 】

ここで発行者鍵変更情報は、I C カード 3 に記録された発行者鍵を変更する情報である。

【 0 0 2 9 】

図 8 に示すように、発行者鍵変更情報作成部 9 は、第 1 の暗号化部 9 A において、新たに I C カード 3 に記録する発行者鍵（以下、新発行者鍵と呼び、この新発行者鍵との対比によりそれまで I C カード 3 に記録されている発行者鍵を旧発行者鍵と呼ぶ）を旧発行者鍵により暗号化して第 1 の鍵変更情報 K 1 を生成する。さらに発行者鍵変更情報作成部 9 は、第 2 の暗号化部 9 B において所定の定数

を新発行者鍵により暗号化し、さらに続く第3の暗号化段9Cにおいて、この第2の暗号化部9Bによる暗号化結果を旧発行者鍵により暗号化して第2の変更情報K2を生成する。発行者鍵変更情報作成部9は、これら第1及び第2の発行者鍵情報K1及びK2を所定の順序で配列して発行者鍵変更情報を生成する。

【0030】

各事業者4A、4B、……は(図2)、例えばコンピュータ等の端末装置12によりリーダライタ11の動作を制御して、このようにして発行者5から発行されるファイル登録情報、アクセス鍵情報、発行者鍵変更情報によりICカード3をアクセスすると共に、アクセス結果を処理する。

【0031】

ここでリーダライタ11は、送信に供する情報を所定の搬送波により変調して内蔵のアンテナを駆動することにより、所定周期で繰り返しICカード3に呼びかけを発する。ここでICカード3がアンテナに近接してこの呼びかけに対する応答がICカード3により送信されると、リーダライタ11は、ICカード3に相互認証を要求する。リーダライタ11は、この相互認証により、ICカード3との間で相互にデータ通信可能な対象であるか否か判断する。

【0032】

このようにして相互認証によりデータ交換可能な対象と判断された場合、リーダライタ11は、端末装置12にデータ交換可能である旨通知し、端末装置12の制御によりICカード3との間で種々のデータを交換する。

【0033】

端末装置12は、このようにしてICカード3との間でデータ交換可能な旨、リーダライタ11より通知されると、リーダライタ11を介してICカード3にアクセスコマンドを送信することにより、各事業者4A、4B、……のためにICカード3に確保されたメモリ空間をアクセスし、さらにアクセス結果によりメモリ空間を更新する。これにより端末装置12においては、例えば事業者がICカード3によりプリペイドカードシステム、さらには電子マネーによるサービスを展開する場合には、ICカード3に記録された金額を検出し、ユーザーにより使用された金額をこの残金より減額してICカード3に記録する等の処理を実行

する。また事業者がユーザーの購入金額に対してポイントを発行すると共に、このポイントに応じた種々のサービスを展開する場合、ユーザーが購入した金額に応じてＩＣカード３に記録されたポイントを更新する等の処理を実行する。

【 0 0 3 4 】

これらのアクセスの処理において、端末装置１２は、ＩＣカード３からの要求により、発行者５より発行されたアクセス鍵を用いてＩＣカード３との間でさらに相互認証の処理を実行する。さらにこの相互認証によるＩＣカード３の処理により、この事業者に設定されたメモリ空間のみアクセスする。

【 0 0 3 5 】

すなわち図９に示すように、端末装置１２は、リーダライタ１１を介してＩＣカード３にアクセスコマンドを発行すると、ＩＣカード３から乱数Ｒを受信する。端末装置１２は、暗号化部１２Ａにおいて、アクセス鍵を用いてこの乱数Ｒを暗号化し、リーダライタ１１を介してこの暗号化結果をＩＣカード３に送出する。端末装置１２は、この暗号化結果のＩＣカード３における解析結果によりＩＣカード３より成功の応答が得られると、この場合、後述するようにＩＣカード３にこの事業者用のメモリ空間が確保されていることにより、先に発行したアクセスコマンドによる処理を継続可能とされる。

【 0 0 3 6 】

ところでこのような相互認証によりＩＣカード３から認証困難を意味するエラーの応答が得られた場合、この場合ＩＣカード３においては、未だこの事業者用にメモリ空間が確保されていないことになる。

【 0 0 3 7 】

この場合端末装置１２は、リーダライタ１１を介して発行者５より取得したファイル登録情報をＩＣカード３に送出し、これによりＩＣカード３にこの事業者用のメモリ空間を確保する。かくするにつき、この場合、端末装置１２は、ＩＣカード３にメモリ空間を確保すると、図９について上述した相互認証の処理を改めて実行した後、対応するメモリ空間をアクセスすることになる。

【 0 0 3 8 】

これに対して発行者５より発行者鍵変更情報、新アクセス鍵が通知され、これ

らの情報により IC カード 3 の更新が指示された場合、このような一連の処理の前に、又は処理の後に、リーダライタ 1 1 を介してこれら発行者鍵変更情報を IC カード 3 に通知する。なお端末装置 1 2 は、例えば一定の移行期間の間にあつては、新アクセス鍵による相互認証結果と、旧アクセス鍵による相互認証結果とにより、未だ IC カード 3 の発行者鍵が新たな発行者鍵に更新されていないと判断された場合に、発行者鍵変更情報を IC カード 3 に通知する。

【 0 0 3 9 】

図 1 に示すように、IC カード 3 は、リーダライタ 1 1 に近接して保持されると、このリーダライタ 1 1 により非接触でアクセスできるように構成されたメモリカードであり、各ユーザーが携帯して使用できるようになされている。

【 0 0 4 0 】

すなわち IC カード 3 においては、リーダライタ 1 1 より送信されたデータを受信し、またリーダライタ 1 1 に所望のデータを送信する信号処理回路と、この信号処理回路で受信したデータをデータ処理し、また信号処理回路を介してリーダライタ 1 1 の送出するデータを生成するデータ処理回路と、このデータ処理回路の処理に必要なデータを保持するメモリとにより構成される。

【 0 0 4 1 】

IC カード 3 は、この信号処理回路とデータ処理回路とにより通信コマンド解析部 1 3 が構成され、さらにデータ処理回路によりアクセス鍵合成部 1 4、ファイル登録部 1 5、発行者鍵変更部 1 6 が構成される。さらに IC カード 3 は、メモリに発行者鍵 1 7 を保持し、さらにこのメモリによりファイル記憶部 1 8 を構成する。

【 0 0 4 2 】

ここでファイル記憶部 1 8 は、各事業者 4 A、4 B、……に割り当てられるメモリ空間と、ファイル鍵 2 0 A～2 0 C を記録するメモリ空間とを構成する。ファイル記憶部 1 8 は、ファイル登録情報に割り当てられたファイル名、ファイルサイズによりダミーデータが記録されることにより、ファイル登録情報による事業者に対してメモリ空間が割り当てられ、さらにこのダミーデータによるファイルが更新されて各事業者でこのメモリ空間を自由に使用できるよう構成される。

さらにファイル記憶部 1 8 は、このようにして確保したメモリ空間と関連付けてファイル鍵 2 0 A、2 0 B、2 0 C が記録される。

【 0 0 4 3 】

通信コマンド解析部 1 3 は、リーダライタ 1 1 に近接して保持されてアンテナに高周波信号が誘起されると、この高周波信号を信号処理してリーダライタ 1 1 より送出されたデータを受信する。この場合リーダライタ 1 1 においては、繰り返し呼びかけを送出していることにより、通信コマンド解析部 1 3 は、この呼びかけを受信すると対応する応答をリーダライタ 1 1 に送出する。さらに通信コマンド解析部 1 3 は、続いてリーダライタ 1 1 との間で相互認証の処理を実行し、ここでリーダライタ 1 1 との間で相互認証の処理を成功すると、リーダライタ 1 1 との間で所望のデータをデータ交換する。

【 0 0 4 4 】

このようなデータ交換において、通信コマンド解析部 1 3 は、リーダライタ 1 1 よりアクセス要求が入力されると、このアクセス要求に付加されたファイル名により、対応するファイル 1 9 A、1 9 B、1 9 C のファイル鍵 2 0 A、2 0 B、2 0 C を用いて、リーダライタ 1 1 との間で相互認証の処理を実行する。

【 0 0 4 5 】

すなわち図 9 に示すように、通信コマンド解析部 1 3 は、リーダライタ 1 1 よりアクセスコマンドを受信すると、乱数 R を生成してリーダライタ 1 1 に送信し、これに応動してリーダライタ 1 1 より送信されるデータを受信する。通信コマンド解析部 1 3 は、アクセスコマンドで要求されたファイルについて、対応するファイル鍵によりアクセス鍵を生成するようにアクセス鍵合成部 1 4 に指示し、この指示によりアクセス鍵合成部 1 4 で生成されたアクセス鍵を取得する。

【 0 0 4 6 】

かくするにつきアクセス鍵合成部 1 4 は、通信コマンド解析部 1 3 の指示により、発行者 5 におけるアクセス鍵合成部 8 と同一の手法によりアクセス鍵を生成して出力する（図 6 参照）。通信コマンド解析部 1 3 は、復号化部 1 3 A において、アクセス鍵合成部 1 4 で生成したアクセス鍵によりリーダライタ 1 1 より出力されるデータの暗号化を解除し、判定部 1 3 B により元の乱数 R と一致するか

否か判断する。これにより通信コマンド解析部 1 3 は、事業者 4 A について認証の処理を実行し、事業者 4 A がアクセスコマンドにより特定されたファイルをアクセスする権限を有しているものに限り、このアクセスコマンドを実行する。すなわちこのアクセスコマンドが対応するファイルの内容をロードする場合、このファイルの内容をリーダライタ 1 1 に送信し、またこのファイルの内容を更新する場合には、続いてリーダライタ 1 1 より送信されるデータによりファイルの内容を更新する。

【 0 0 4 7 】

これに対して通信コマンド解析部 1 3 は、例えば未だこの事業者 4 A についてメモリ空間が確保されていない場合、すなわちファイル記憶部 1 8 にこのアクセスコマンドによるファイルが登録されていない場合、リーダライタ 1 1 にエラーの応答を通知する。これによりこのアクセスコマンドに係る事業者がこの IC カード 3 の利用を発行者 5 と契約している事業者 4 A の場合、リーダライタ 1 1 よりファイル登録情報が送信され、通信コマンド解析部 1 3 は、このファイル登録情報を受信することになる。なおこのようなアクセス時に代えて、発行者 5 における IC カード 3 発行時等において、事前に所定の事業者についてメモリ空間を確保する場合、同様にファイル登録情報を受信することになる。

【 0 0 4 8 】

このようにしてファイル登録情報を受信すると、通信コマンド解析部 1 3 は、図 1 0 に示すように、第 1 の暗号化部 1 3 C において、ファイル登録情報に割り当てられたファイル名、ファイルサイズの情報を発行者鍵 1 7 により暗号化し、続く排他的論理和演算部 1 3 D によりこの暗号化結果とファイル登録情報に割り当てられたファイル鍵情報とで排他的論理和を演算する。さらに第 2 の暗号化手段 1 3 E において、発行者鍵を用いてこの排他的論理和の演算結果を暗号化してチェックコードを生成する。

【 0 0 4 9 】

通信コマンド解析部 1 3 は、このようにして生成したチェックコードと、ファイル登録情報に割り当てられたチェックコードとを比較部 1 3 F で比較し、この比較結果によりファイル記憶部 1 8 に事業者のメモリ空間を確保する。

【 0 0 5 0 】

すなわち図 1 1 に示すように、通信コマンド解析部 1 3 は、ステップ S P 1 からステップ S P 2 に移ってファイル登録情報を受信した後、続くステップ S P 3 において、図 1 0 で説明したようにしてチェックコードを確認し、ここで否定結果が得られると、ステップ S P 4 に移り、リーダライタ 1 1 にエラーの応答を送信した後、ステップ S P 5 に移ってこの処理手順を終了する。

【 0 0 5 1 】

これに対してチェックコードが一致した場合、ステップ S P 3 からステップ S P 6 に移り、このファイル登録情報によりファイル記憶部 1 8 にファイルを記録する。ここで通信コマンド解析部 1 3 は、ファイル登録部 1 5 を起動し、ファイル登録情報に割り当てられたファイル名、ファイルサイズにより所定のダミーデータをファイル記憶部 1 8 に記録してメモリ空間を確保する。さらにこのファイル登録情報に割り当てられたファイル鍵をこのファイルと関連付けてファイル記憶部 1 8 に記録する。かくするにつきファイル登録部 1 5 は、このようなファイル登録情報によるファイルをファイル記憶部 1 8 に記録する処理を実行する。

【 0 0 5 2 】

これにより I C カード 3 においては、図 1 2 に示すように、特定事業者にのみアクセス可能なファイルがファイル登録情報と共にメモリに記録されることになる。

【 0 0 5 3 】

これに対して図 1 3 に示すように、発行者鍵変更情報がリーダライタ 1 1 より入力された場合、通信コマンド解析部 1 3 は、この発行者鍵変更情報を発行者鍵変更部 1 6 に渡し、この発行者鍵変更部 1 6 による処理結果をリーダライタ 1 1 に通知する。

【 0 0 5 4 】

ここで発行者鍵変更部 1 6 は、図 1 4 に示すように、この発行者鍵変更情報を第 1 及び第 2 の鍵変更情報 K 1 及び K 2 に分離した後、復号化部 1 6 A において、保持した発行者鍵（旧発行者鍵である）により第 1 の鍵変更情報 K 1 を処理して新発行者鍵を復号する。さらに復号化部 1 6 B において、旧発行者鍵により第

2の鍵変更情報K2を処理した後、続く復号化部16Cにおいて、新発行者鍵により処理し、これにより発行者鍵変更情報の生成時に設定した定数を再生する（図8）。発行者鍵変更部16は、続く判定部16Dにより、このようにして再生した定数が発行者鍵変更情報の生成時に設定した定数か否か判定する。

【0055】

発行者鍵変更部16は、この判定において不一致の判定結果が得られると、通信コマンド解析部13に通知し、これによりICカード3では、リーダライタ11に不成功の応答を送出する。これに対して一致の判定結果が得られると、通信コマンド解析部13に通知し、これによりICカード3では、リーダライタ11に成功の応答を送出する。

【0056】

さらに発行者鍵変更部16は、一致の判定結果が得られると、この発行者鍵変更情報を処理して検出された新発行者鍵によりメモリに保持した発行者鍵17を更新する。これによりICカード3では、図15に示すように、発行者鍵変更情報を発行して発行者鍵を変更した後、新たなアクセス鍵により対応するメモリ空間をアクセスできるようになされている。

【0057】

（1-2）第1の実施の形態の動作

以上の構成において、このICカードシステム1においては（図1～図3）、このシステムの管理部門としての発行者5から、管理部門に固有の発行者鍵が記録されてICカード3が発行される。

【0058】

その一方で、発行者5において、このICカード3を用いて自己のサービスを提供したいと望む事業者4A、4B、……に対して、事業者4A、4B、……に固有のファイル鍵情報を発行者鍵により暗号化したアクセス鍵が生成されて配付される（図6）。さらに各事業者4A、4B、……に割り当てるメモリ空間をファイルにより特定可能に、このファイルのファイル名及びファイルサイズの情報が発行者鍵により暗号化されてチェックコードが生成され（図5）、このチェックコード、ファイル名及びファイルサイズの情報、ファイル鍵情報によるファイ

ル登録情報が各事業者 4 A、4 B、……に提供される。

【 0 0 5 9 】

ICカードシステム 1 においては、このファイル登録情報を ICカード 3 に送信すると、ICカード 3 において、ファイル登録情報の作成時と同様に発行者鍵を基準にしてチェックコードが作成され、このチェックコードがファイル登録情報に割り当てられたチェックコードと一致するか否か判定され（図 1 0 ～図 1 2）、これによりこのファイル登録情報が正しく発行者 5 より発行されたものか否か判定される。さらにファイル登録情報が正しく発行者 5 より発行されたものの判断できる場合、このファイル登録情報に割り当てられたファイル名、ファイルサイズによりダミーデータを記録して、このファイル登録情報に係る事業者用に ICカード 3 のメモリ空間がファイル名によりアクセス可能に確保される。またこのメモリ空間をアクセスできるように、このファイル名と関連付けてファイル鍵情報が記録される。

【 0 0 6 0 】

このとき ICカードシステム 1 においては、チェックコードを用いてファイル登録情報が正しく発行者 5 より発行されたものか否か判定することにより、例えば特定の事業者がファイル登録情報作成してこの ICカードシステムを無断で使用するような不正な行為、さらにはこの ICカード 3 の内容を改修する等の行為を防止することができる。

【 0 0 6 1 】

これに対してこのようにしてメモリ空間が事業者用に確保された後において、各事業者において ICカード 3 にアクセスコマンドが入力されると、ICカード 3 より乱数 R が送信され（図 9）、事業者側においては、この乱数 R をアクセス鍵により暗号化して ICカード 3 に送信する。ICカード 3 においては、アクセスコマンドに付加されたファイル名に対応するファイル鍵情報により受信したデータを復号し、送信した乱数 R と一致するか否か判定することにより、この事業者がこのファイルのアクセスを許される正しい事業者か否か判定される。さらに正しい事業者と判断される場合には、アクセスコマンドに対応してこのファイルの内容を事業者に送信し、またこのファイルの内容が更新される。

【0062】

これによりこのICカード3を共用する各事業者においては、ICカード3に記録した自己のファイル名によりICカード3を単にアクセスして、ICカード3の要求によりファイル鍵情報によりICカード3から送信されたデータを暗号化して送り返すだけで相互認証の処理が完了し、あたかもこのICカード3がこの事業者に専用のメモリカードかのように使用することができる。またこのようなファイル鍵情報により事業者を認証して処理することにより、他の事業者によるファイルの盗み見を防止でき、さらにはこの他の事業者によるファイルの改修等の防止することができる。これによりICカードシステム1では、このICカード3を複数の事業者で共用することができる。

【0063】

また乱数Rをアクセス鍵情報により暗号化して送受することにより、アクセス鍵情報自体については、外部への漏洩を防止でき、これによってもセキュリティを向上することができる。

【0064】

またICカード3に記録されたファイルに対応するファイル鍵情報自体についても、ICカード3に保持されたままで処理されることにより、さらにはファイル鍵情報よりアクセス鍵情報を生成し、このアクセス情報が事業者に手渡されることにより、事業者に対してもファイル鍵情報を秘密にすることができ、これらによってもセキュリティを向上することができる。

【0065】

さらにこのような処理の前提である発行者鍵については、管理部門である発行者5のみが知り得、かつ管理でき、また事業者においても発行者鍵を何い知ることが困難のようにアクセス鍵情報が生成されて発行されていることにより、例えば特定の事業者がこのICカード3のメモリ空間を契約以上の大きさにより無断で使用するような不正な行為、さらにはこのICカード3の内容を改修する等の行為を防止することができる。

【0066】

ところでこのようにしてICカード3を使用している状態で、セキュリティ

を図る上でも、発行者鍵を定期的に変更することが必要になる。また契約の更新を望まない事業者も存在することが考えられることにより、この場合この事業者がＩＣカード３を使用できないようにすることも必要となる。

【 0 0 6 7 】

このためＩＣカードシステム１では、発行者５において、定期的に、新たな発行者鍵、所定の定数を古い発行者鍵により暗号化して発行者鍵変更情報が生成され（図８）、この発行者鍵変更情報が各事業者に提供される（図７）。またこの発行者鍵変更情報に対応するファイル鍵情報が各事業者に提供される。さらにこの事業者よりＩＣカード３にこの発行者鍵変更情報が送信される（図１３）。ＩＣカード３においては、古い発行者鍵によりこの発行者鍵変更情報の暗号が解除されて新たな発行者鍵、所定の定数が復号化され、この所定の定数によりこの発行者鍵変更情報が発行者５により正しく発行されたものか否か判断される（図１４）。さらに発行者５により正しく発行されたものと判断される場合には、それまでの発行者鍵が新たな発行者鍵により更新される。

【 0 0 6 8 】

これによりＩＣカードシステム１では、このＩＣカード３をそれまでアクセス可能であった事業者であっても、この新たな発行者鍵に対応するファイル鍵情報によらなければ、ＩＣカード３をアクセスすることが困難となる。

【 0 0 6 9 】

このようにして発行者鍵を更新するにつき、ＩＣカードシステム１では、新たな発行者鍵及び所定の定数をそれぞれ古い発行者鍵により暗号化して発行者鍵変更情報Ｋ１、Ｋ２を生成し、この定数により発行者鍵変更情報が発行者５により正しく発行されたものか否か判断することにより、不正な発行者鍵の変更を防止することができ、これによりＩＣカードシステム１の信頼性を確保することができる。

【 0 0 7 0 】

（１－３）実施の形態の効果

以上の構成によれば、発行者鍵情報とファイル鍵情報により生成されたアクセス鍵を各事業者に配付し、このアクセス鍵を利用した認証によりＩＣカード３を

アクセス可能とすることにより、複数の事業者でＩＣカードを共用することができる。

【 0 0 7 1 】

また各事業者が使用するファイル名、各事業者に確保するメモリ空間の大きさを特定するファイルサイズの情報が発行者鍵により暗号化してファイル登録情報を生成し、このファイル登録情報によりメモリ空間を確保することにより、事業者の要望に応じたメモリ空間を各事業者に提供することができる。またファイル名を基準にしたアクセスである簡易なアクセス処理により、自己に割り当てられたメモリ空間をアクセスすることができる。

【 0 0 7 2 】

またファイル名、ファイルサイズの情報が発行者鍵により暗号化して生成したチェックコードにファイル名、ファイルサイズ情報を付加してファイル登録情報を生成することにより、例えば特定の事業者がこのＩＣカード３のメモリ空間を契約以上の大きさにより無断で使用するような不正な行為、さらにはこのＩＣカード３の内容を改修する等の行為を防止することができる。

【 0 0 7 3 】

また古い発行者鍵により新たな発行者鍵を暗号化して発行者鍵変更情報を生成し、この発行者鍵変更情報によりＩＣカード３に保持した発行者鍵を更新することにより、セキュリティを図ることができ、また契約の更新を望まない事業者の使用を禁止することができる。

【 0 0 7 4 】

(2) 第 2 の実施の形態

図 1 6 は、図 8 との対比により、本発明の第 2 の実施の形態に係るＩＣカードシステムにおいて、発行者におけるアクセス鍵合成部の構成を示すブロック図である。この実施の形態に係るＩＣカードシステムでは、このアクセス鍵合成部 2 8 と関連する構成が異なる点を除いて第 1 の実施の形態と同一に構成される。

【 0 0 7 5 】

ここでこのＩＣカードシステムでは、発行者において 2 つの発行者鍵 A 及び発行者鍵 B により 2 種類のアクセス鍵 A 及びアクセス鍵 B を生成する。すなわち A

アクセス鍵合成部 2 8 は、暗号化部 2 8 A において発行者鍵 A を発行者鍵 B により暗号化し、続く暗号化部 2 8 B において、暗号化部 2 8 A の暗号化結果を事業者鍵により暗号化してアクセス鍵 A を生成する。なおここで事業者鍵は、各事業者に固有の鍵情報である。

【 0 0 7 6 】

さらにアクセス鍵合成部 2 8 は、続く暗号化部 2 8 C において、このアクセス鍵 A によりアクセス鍵 A を暗号化してアクセス鍵 B を生成する。発行者は、これらアクセス鍵 A 及びアクセス鍵 B を事業者に渡す。

【 0 0 7 7 】

この 2 つのアクセス鍵 A 及び B に対応して、図 1 7 に示すように事業者の端末においては、乱数 R 1 を生成し、暗号化部 3 1 A において、この乱数をアクセス鍵 A による暗号化する。事業者の端末は、アクセス時、例えばアクセスコマンドと共にこの暗号化部 3 1 A による暗号化結果を IC カードに送信する。

【 0 0 7 8 】

IC カードにおいて、通信コマンド解析部は、第 1 の復号化部 3 2 A において、このようにして伝送された暗号化結果を同一のアクセス鍵 A により処理して乱数 R 1 を復号化する。さらに第 1 のアクセス鍵 A と、アクセスに係るファイルのファイル鍵とから第 2 のアクセス鍵 B を生成し、続く暗号化部 3 2 B において、この第 2 のアクセス鍵 B により復号化部 3 2 A の復号化結果を暗号化して事業者に送信する。

【 0 0 7 9 】

これに対応して事業者においては、このようにして IC カードより送信された情報を第 1 のアクセス鍵 B により復号化部 3 1 B で処理した後、判定部 3 1 C において、元の乱数 R 1 と一致するか否かを判定する。

【 0 0 8 0 】

また IC カード側においては、乱数 R 2 を生成し、暗号化部 3 2 D で第 2 のアクセス鍵 B により暗号化して送信する。これに対応して事業者側においては、復号化部 3 1 D において、アクセス鍵 B により処理して乱数 R 2 を復号し、続く暗号化部 3 1 E においてこの乱数 R 2 をアクセス鍵 A により暗号化して IC カード

に送信する。

【 0 0 8 1 】

ＩＣカード側においては、復号化部 3 2 E において、アクセス鍵 A により乱数 R 2 を復号し、続く判定部 3 2 F において、この復号化結果が元の乱数 R 2 と一致するか否か判断する。

【 0 0 8 2 】

ＩＣカード及び事業者の端末においては、各判定結果により一致結果が得られた場合、相互認証を完了し、メモリ空間へのアクセスを開始する。

【 0 0 8 3 】

図 1 6 及び図 1 7 に示すように、乱数をアクセス鍵による暗号化して送受するようになれば、第 1 の実施の形態について説明した場合のように、認証に供する乱数を直接送受しないで済むことにより、その分安全性を向上することができる。また双方で乱数を生成して確認することにより、これによっても安全性を向上することができる。

【 0 0 8 4 】

(3) 他の実施の形態

なお上述の実施の形態においては、ファイル鍵情報を発行者鍵により暗号化してアクセス鍵を作成する場合について述べたが、本発明はこれに限らず、複数の発行者鍵により多段階で暗号化してアクセス鍵を生成する場合等、要は、第 3 者に秘匿して各事業者固有のファイル鍵情報と管理部門固有の発行者鍵情報により所定の管理部門でアクセス鍵情報生成し、このアクセス鍵情報により事業者の端末とＩＣカードとの間で認証の処理を実行することにより、上述の実施の形態と同様の効果を得ることができる。

【 0 0 8 5 】

また上述の実施の形態においては、ファイル名、ファイルサイズの情報、チェックコードによるファイル登録情報を送受することにより、認証の処理とメモリ空間の確保とを纏めて実行する場合について述べたが、本発明はこれに限らず、例えば個別に事業者を認証した後、メモリ空間の登録を受け付けるようにしてもよい。なおこの場合、事業者固有の鍵情報と、発行者鍵とにより暗号化した所

望の情報を送受して認証の処理を実行した後、別途、ファイル名、ファイルサイズの情報等を事業者に固有の鍵情報と発行者鍵とにより暗号化して作成した情報を送受してメモリ空間を確保することが考えられる。

【 0 0 8 6 】

また上述の実施の形態においては、ファイル登録情報、アクセス情報、発行者鍵変更情報とを同一の発行者鍵により処理する場合について述べたが、本発明はこれに限らず、個別に、発行者に固有の鍵情報を使用して処理するようにしてもよい。

【 0 0 8 7 】

また上述の実施の形態においては、本発明を非接触型のＩＣカードを使用したＩＣカードシステムに適用する場合について述べたが、本発明はこれに限らず、接触型のＩＣカードを使用したＩＣカードシステム、さらにはＩＣカードに限らず、例えば携帯電話等、種々の情報携帯装置を用いたシステムに広く適用することができる。

【 0 0 8 8 】

【発明の効果】

上述のように本発明によれば、管理部門で管理する発行者鍵情報と、事業者に固有のファイル鍵情報によりアクセス鍵を生成して各事業者に配付し、このアクセス鍵を使用して情報携帯装置をアクセスすることにより、複数の事業者でＩＣカードを共用することができる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態に係るＩＣカードシステムを示すブロック図である。

【図 2】

図 1 のＩＣカードシステムの事業者、発行者を詳細に示すブロック図である。

【図 3】

ＩＣカードの発行時の説明に供するブロック図である。

【図 4】

ファイル登録情報の発行時の説明に供するブロック図である。

【図 5】

ファイル登録情報の生成の説明に供するブロック図である。

【図 6】

アクセス鍵の生成の説明に供するブロック図である。

【図 7】

発行者鍵変更情報の発行時の説明に供するブロック図である。

【図 8】

発行者鍵変更情報の生成の説明に供するブロック図である。

【図 9】

アクセス時の処理の説明に供するブロック図である。

【図 1 0】

ファイル登録情報の処理の説明に供するブロック図である。

【図 1 1】

ファイル登録情報の処理手順を示すフローチャートである。

【図 1 2】

ファイル登録情報による処理の説明に供するブロック図である。

【図 1 3】

発行者鍵変更情報による処理の説明に供するブロック図である。

【図 1 4】

発行者鍵変更情報の処理の説明に供するブロック図である。

【図 1 5】

発行者鍵変更情報による処理の説明に供するブロック図である。

【図 1 6】

第 2 の実施の形態に係る I C カードシステムにおけるアクセス鍵の生成の説明に供するブロック図である。

【図 1 7】

図 1 6 の構成によるアクセス鍵の処理の説明に供するブロック図である。

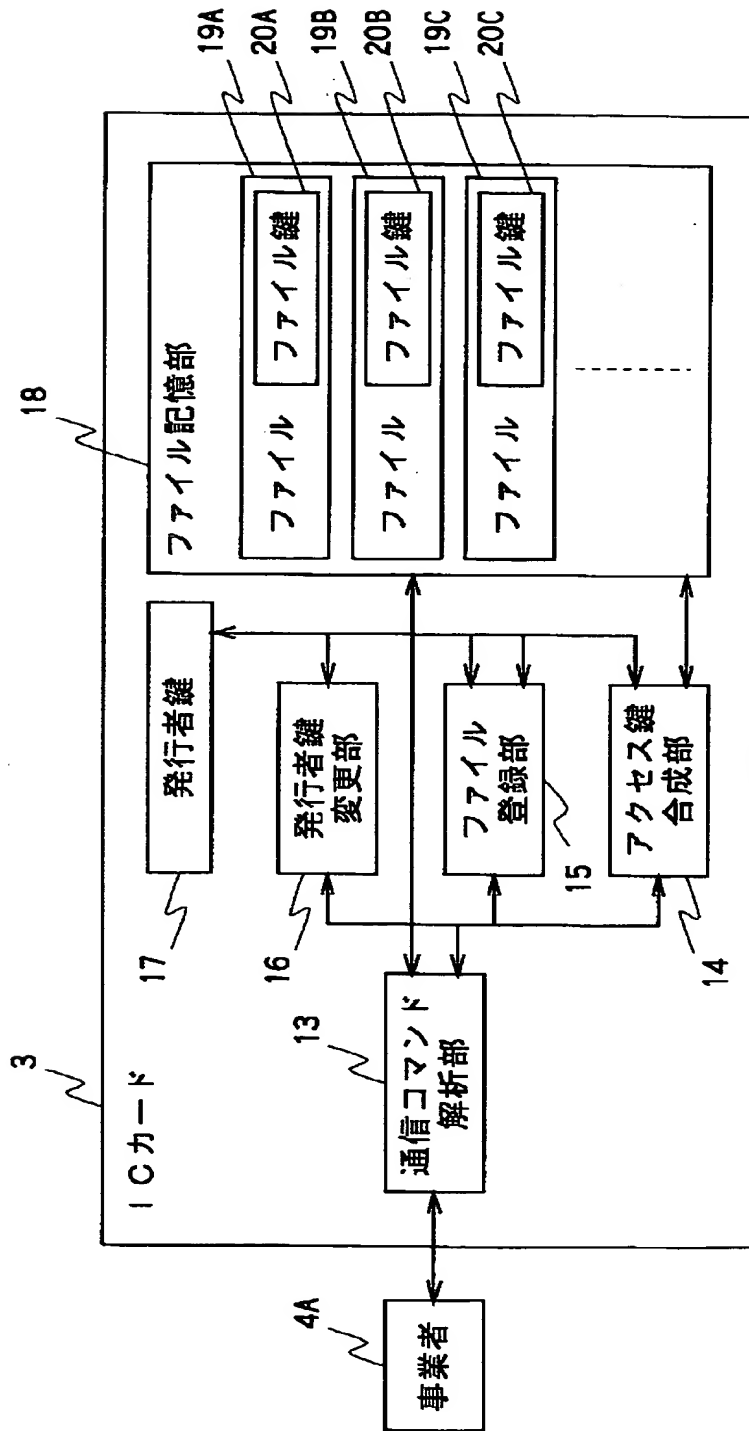
【符号の説明】

1 …… I C カード、 2 …… ユーザー、 3 …… I C カード、 4 A、 4 B …… 事業

者、 5 …… 発行者、 6、 1 2 …… 端末装置

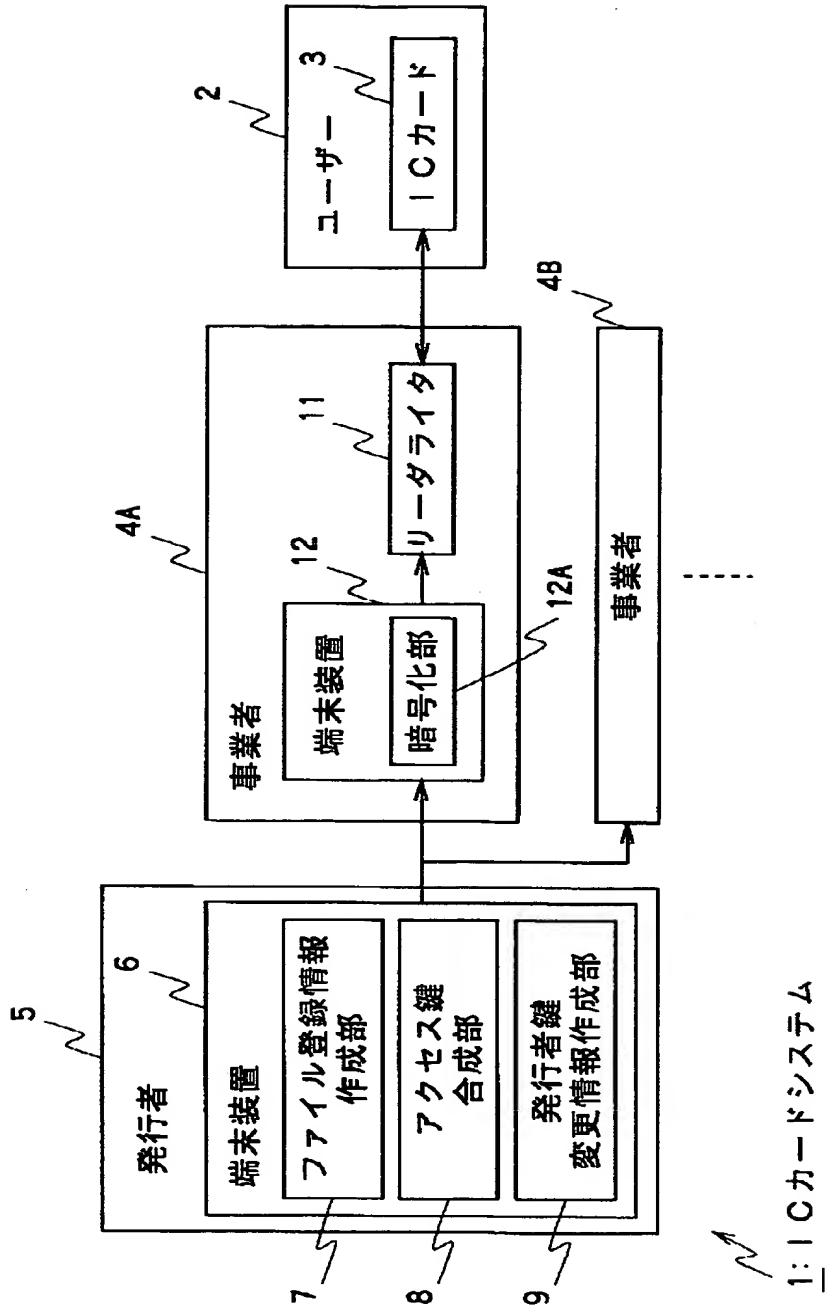
【書類名】 図面

【図1】

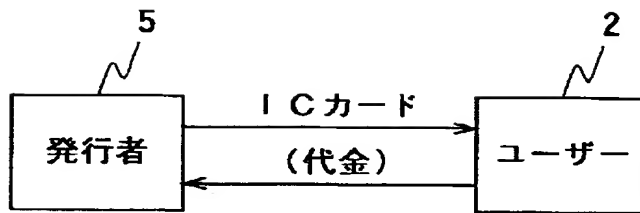


1: ICカードシステム

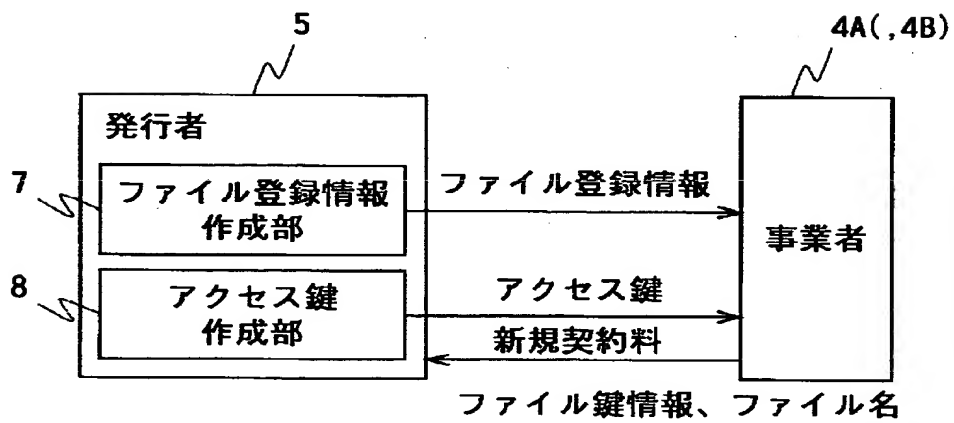
【図2】



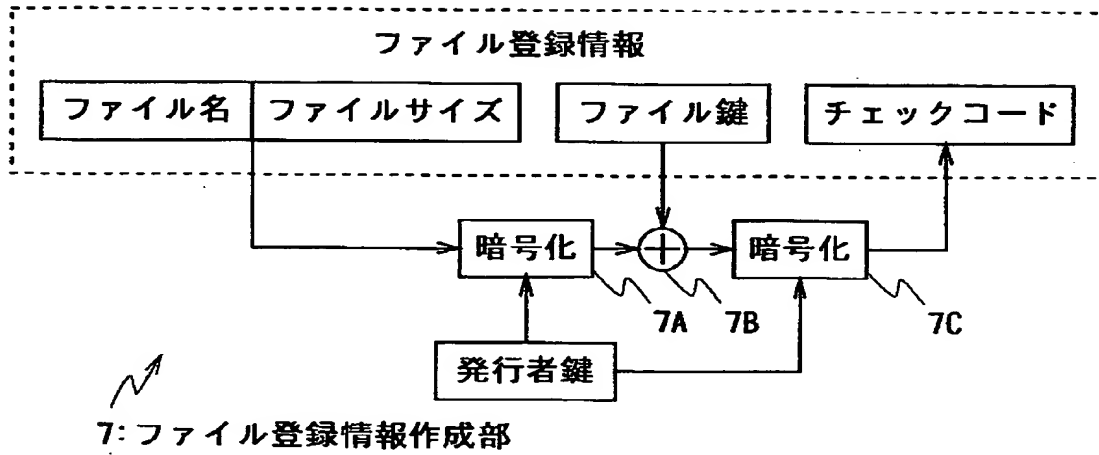
【図 3】



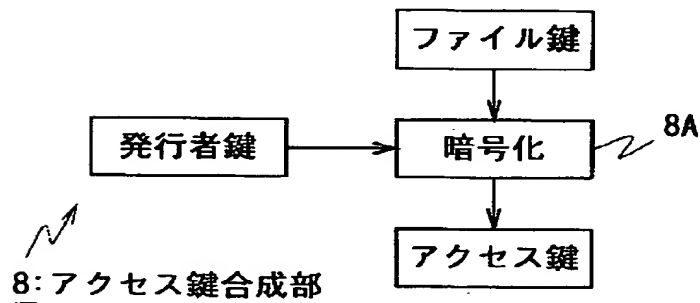
【図 4】



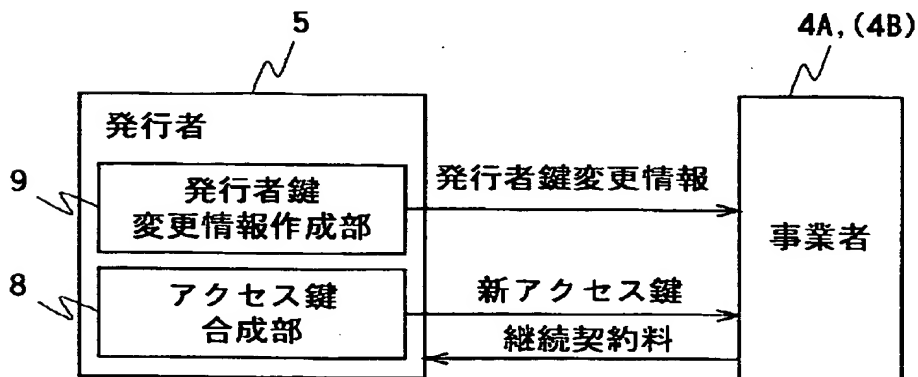
【図5】



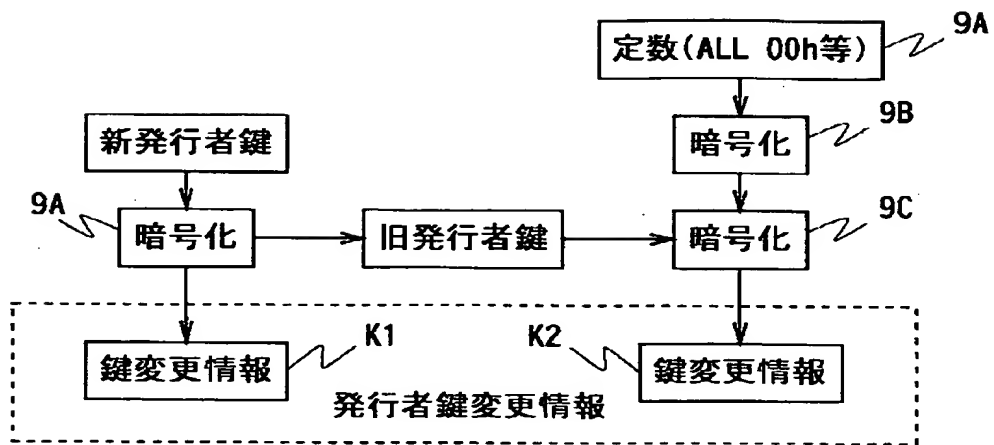
【図6】



【図7】

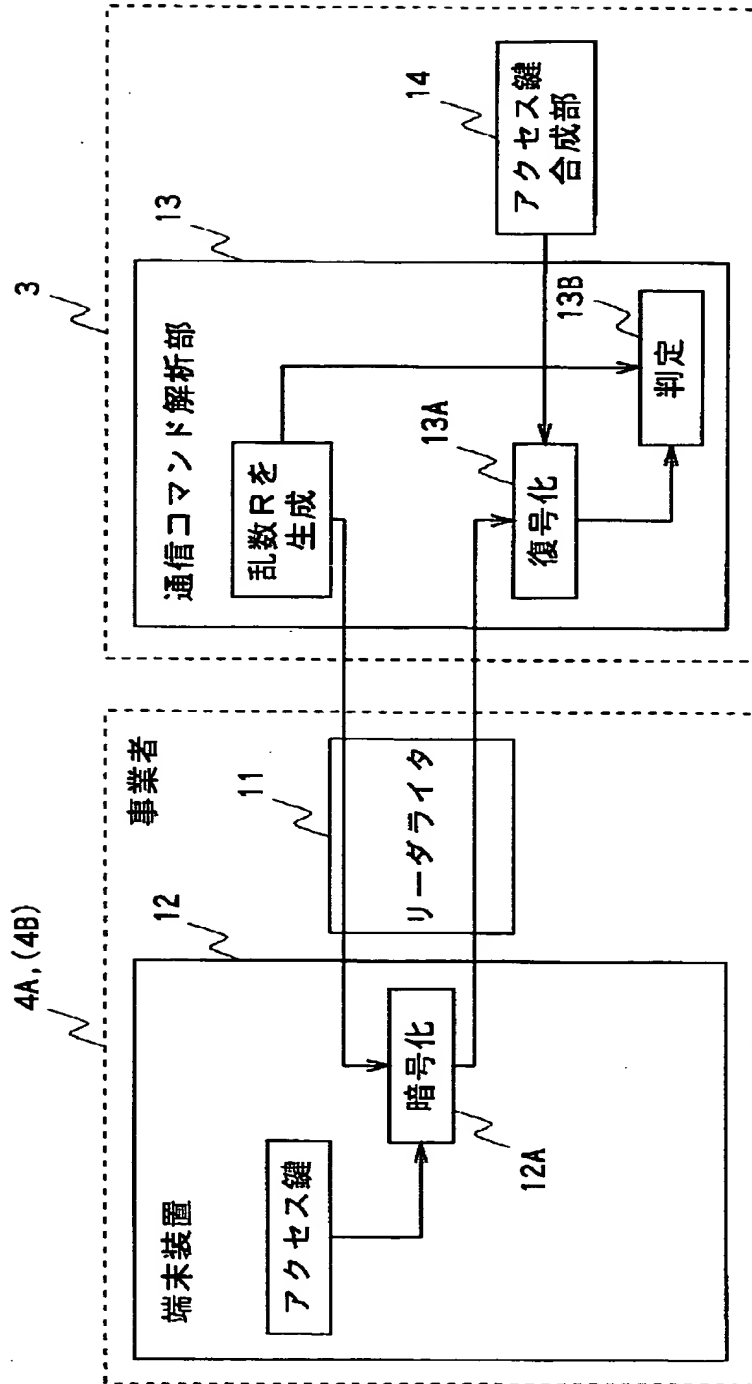


【図 8】

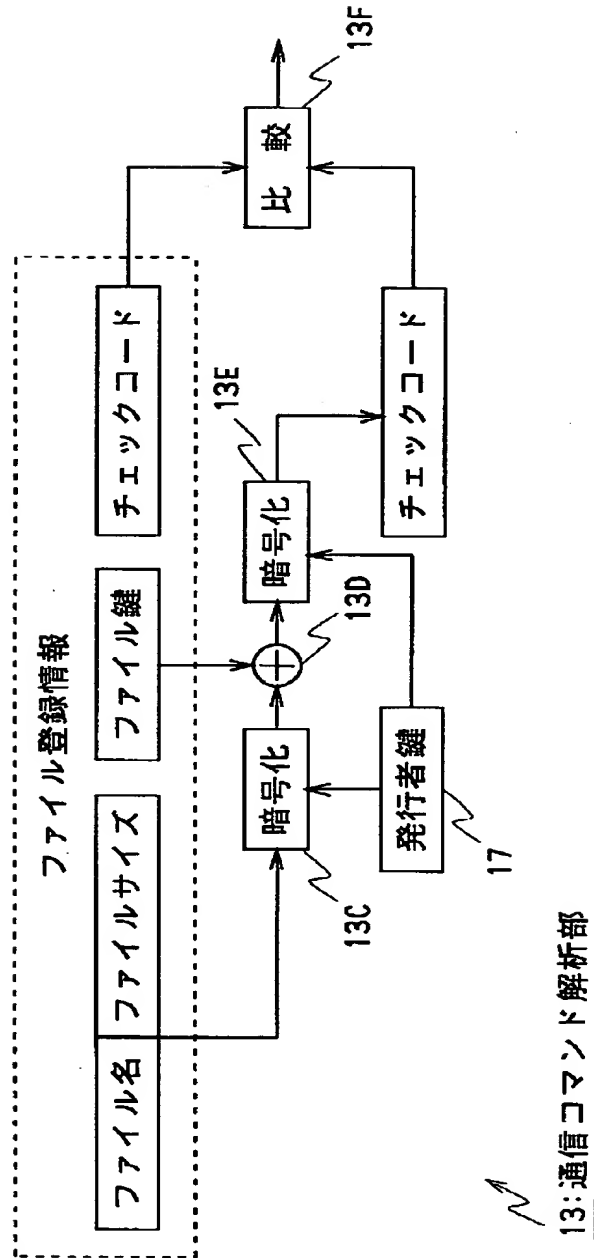


9: 発行者鍵変更情報作成部

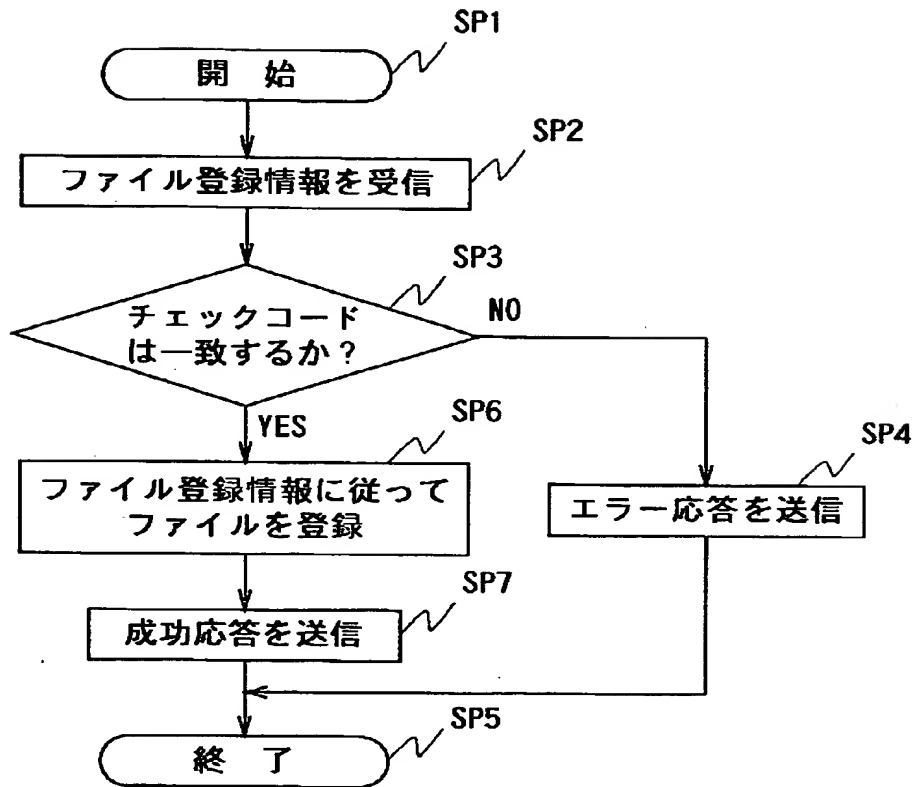
【図 9】



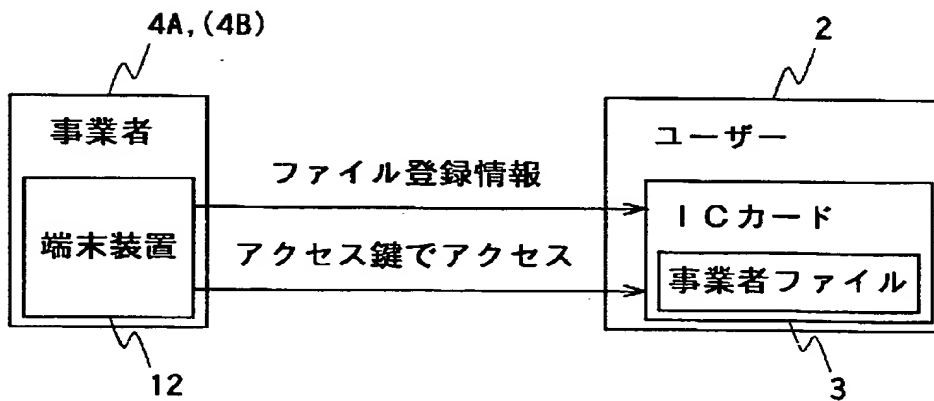
【図10】



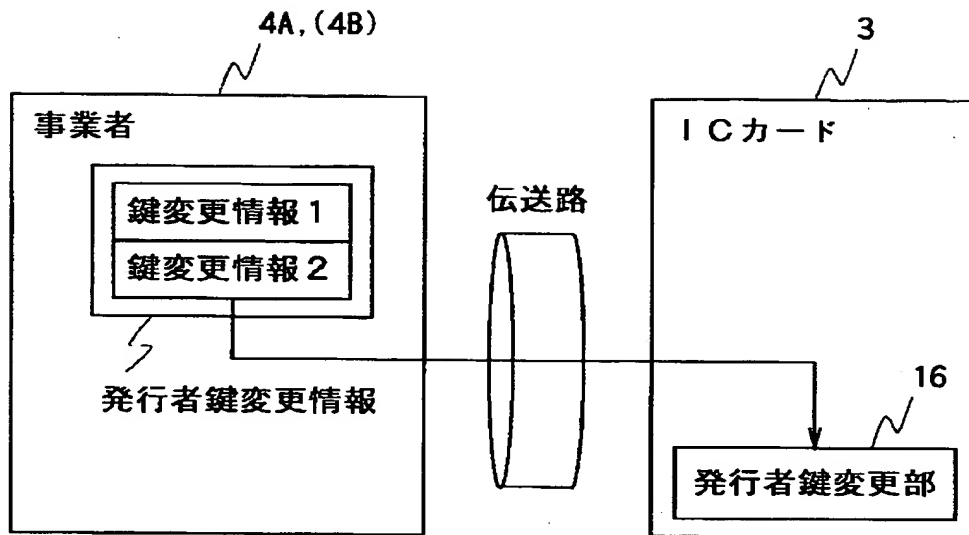
【図 1 1】



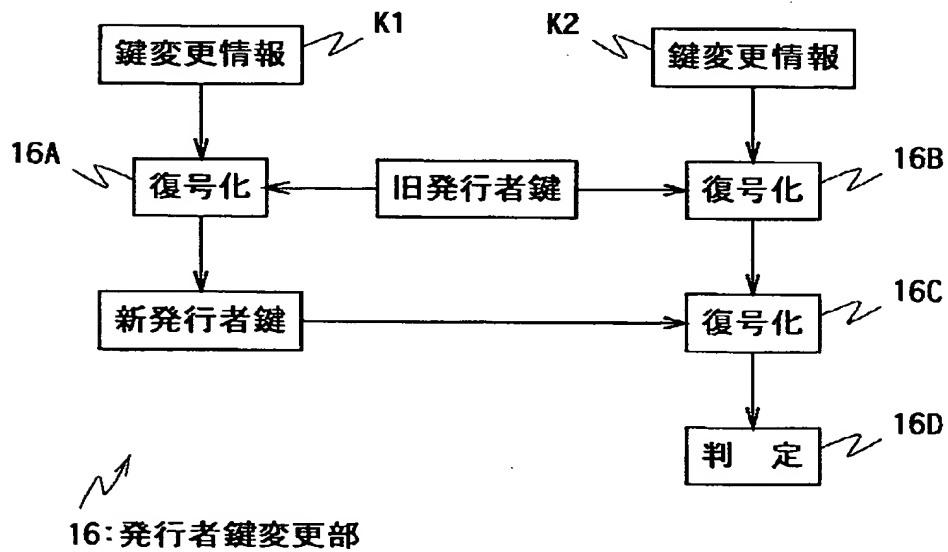
【図 1 2】



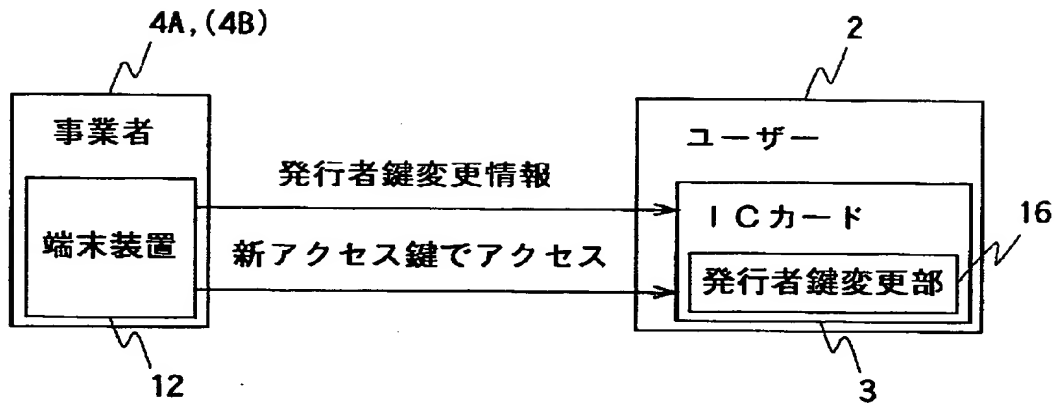
【図 1 3】



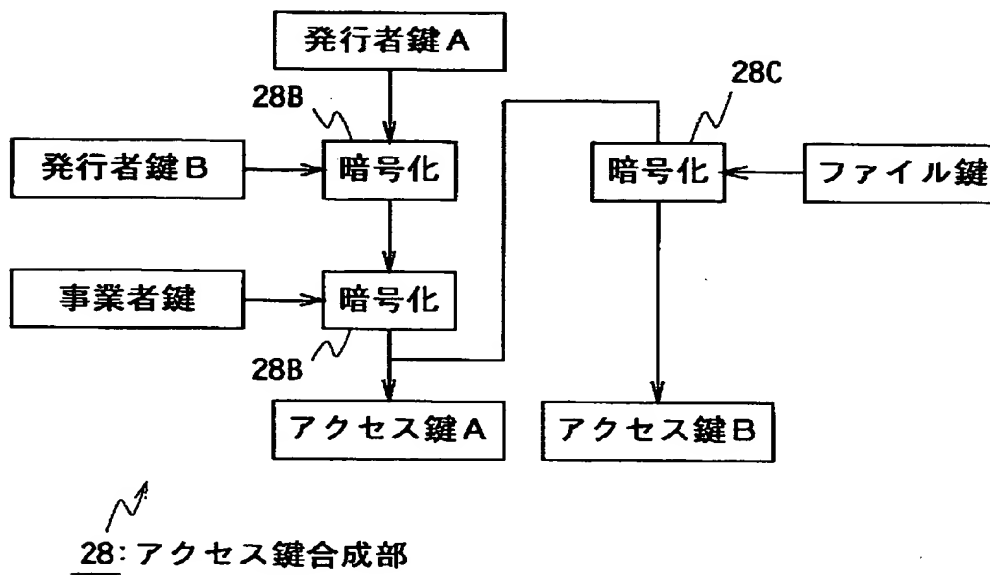
【図 1 4】



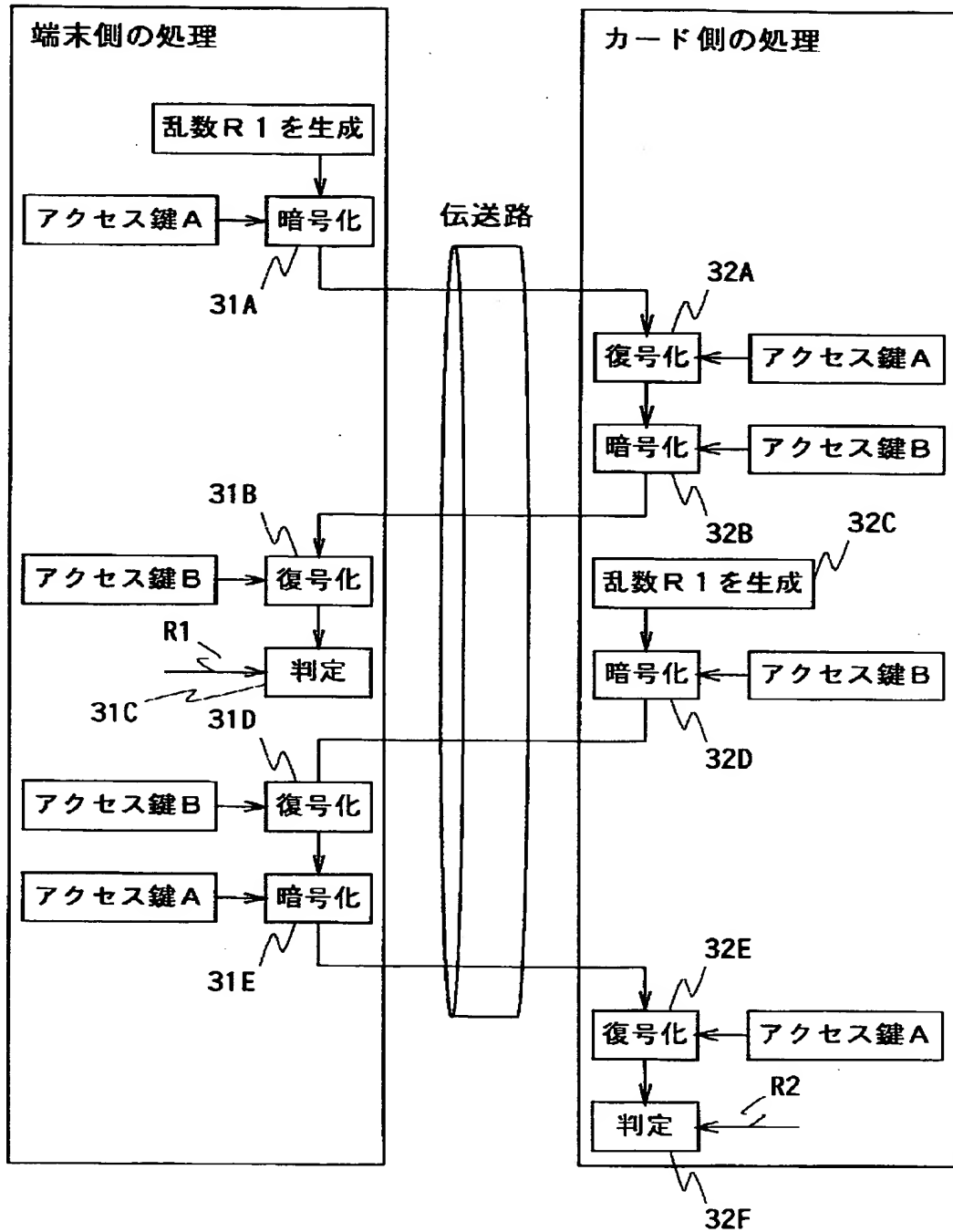
【図 1 5】



【図 1 6】



【図 17】



【書類名】 要約書

【要約】

【課題】 本発明は、情報携帯処理システム、情報携帯装置のアクセス装置及び情報携帯装置に関し、例えば非接触型のＩＣカードを用いたシステムに適用して、複数の事業者でＩＣカードを共用することができるようにする。

【解決手段】 本発明は、管理部門で管理する発行者鍵情報と、事業者に固有のファイル鍵情報によりアクセス鍵を生成して各事業者に配付し、このアクセス鍵を使用して情報携帯装置をアクセスする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社